AIR WAR COLLEGE

AIR UNIVERSITY

NETWORKS—THE AIR FORCE'S NEWEST WEAPON SYSTEMS

by

Von A. Gardiner, Lieutenant Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Stephen Wright

Maxwell Air Force Base, Alabama

17 February 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **17 FEB 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE **Networks - The Air Force's Newest Weapon Systems**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,325 Chennault Circle,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

Too often in the USAF we get caught-up with the issues surrounding technological, operational capabilities, job security and self-preservation, ignoring the basic organizational constructs that facilitate employment of information technologies (IT) and mission accomplishment. We also have a tendency to become servants to “technology,” always seeking to field the latest and greatest IT innovations without fully acknowledging and assessing applicability to the underlying principles or doctrine that actually make or break the mission. Arguably, the single most critical factor that leadership can influence to ensure mission objectives are met is the proactive management of strategic organizational change and organizational interdependence providing "holistic" cohesion and operational autonomy. This analysis argues that the creation, transformation and operational effectiveness of USAF organizations in an increasingly turbulent environment depend upon the development and effective employment of a dynamic change management strategy for aligning the organizational structure with environmental factors and for creating symbiotic inter-organizational relationships. The organizational structure has always been a fundamental enabler for operational success.

This analysis seeks to refocus Air Force leadership on the importance of ensuring organizational constructs adequately support existing and emerging mission objectives. I hope this analysis provides compelling rationale for the need to perform strategic organizational change management on a continual basis; thus eliminating the ad hoc approach currently employed for network engineering design and the development of CONOPS, doctrine and tactics, techniques and procedures.

Finally, I’d like to acknowledge the efforts of Colonel David Gruber (USAF-retired), Colonel Stephen Wright, Mr. Robert Kaufman (Lieutenant Colonel, USAF-retired), Major Eric Oliver, Captain Austin Hood and Mr. Tony Storace for the information and support they provided me in thinking through this organizational construct. Their unique insights into how organizations should be aligned in order to better support mission operations and deliver Information Superiority to the warfighter contributed significantly towards the completion of this analysis.

Abstract

The current USAF organizational construct for network weapon systems is out of date, inefficient and does not adequately support emerging Information Operations objectives. Specifically, we have independent organizations functioning under completely different chains of command focused on the very same mission sets and objectives. As a result, the Air Force organizational structure, with respect to most network-related activities and operations, is fractured and extremely inefficient. Furthermore, the USAF does not have a centralized authority responsible to orchestrate collaboration and synergy among the various entities responsible for network concept of operations development, engineering and design, procurement, technician training, tactics, techniques and procedures or doctrine. As a result of what may be view as parochialism or self-preservation, several of these 'should-be' interdependent organizations in fact operate in vacuums, functioning on unsynchronized timelines as self-serving, independent entities. These organizations suffer from what has been referred to as operational and organizational myopia. They remain so functionally or organizationally compartmented and internally focused, working their own respective agendas, that they in fact marginalized their own operational and institutional value to the larger USAF. Although the Air Force is in the midst of transforming the organizational structure to better support networks at the operational level by establishing an AFNetOps Command to oversee and coordinate all network operations under an architecture-based construct, it is not addressing the need to overhaul and realign at the strategic and tactical levels. In essence, the USAF is building a new operational structure on a fractured foundation and is likely destined to deliver sub-optimum results.

Chapter 1

Introduction

Today's fast-paced aerospace operational environment is highly complex, lethal and information technology (IT) dependent. In order to maintain the operational edge over would-be foes, the U.S. Air Force (USAF) has become increasingly dependent on state-of-the-art networks of all types and sizes. This dependence upon networks and the information they transport, which has profound advantages for the U.S. military, is also a double-edged sword. Although viewed as tremendous force enablers and multipliers, it suggests that the United States is also vulnerable to attack by determined adversaries and raises questions about network-related Concept of Operations (CONOPS), doctrine, tactics, techniques and procedures (TTP) and ultimately the USAF's ability to conduct military operations via networks.

In 1998, as a result of operational dependencies, networks were declared "weapon systems."[1] According to Brigadier General Dale Meyerrose, the Air Combat Command Director of Communications and Information, USAF leadership fully expected the same or similar organizational constructs and well-established design criteria and fielding processes demanded of other weapon systems would now be applied to networks.[2] No longer would ad hoc processes and/or home-grown network solutions be funded or tolerated. The basic intent was to raise the level of operational importance and priority of networks to ensure they competed on a level playing field with other weapon systems.

[1] General Richard E. Hawley, Commander, Air Combat Command (address, Promotion ceremony at Langley AFB, VA, 1 October 1998).
[2] Brigadier General Dale W. Meyerrose, Air Combat Command, Director of Communications and Information (Based on follow-up discussion with his staff after COMACC declared networks weapon systems, Langley AFB VA, 1998).

Unfortunately, some eight years after being classified as weapon systems, the trend continues and networks are still designed, engineered, fielded and funded in an ad hoc fashion and treated like information plumbing. The fact is, from design to procurement to fielding to training to sustainment, networks are consistently treated purely as enablers, not legitimate weapon systems. Aside from “networks,” one would be hard pressed to identify another weapon system the Air Force has fielded in the past twenty years that was not designed and/or upgraded to satisfy legitimate, well-documented operational gaps or shortfalls and was not preceded by a well-vetted CONOPS and associated doctrine.

The USAF’s feverish effort to field wireless networks across the service is the most recent example of this trend. While there are obvious fiscal and operational benefits associated with the employment of wireless technologies, there are also many inherent operational and security risks. However, to date there is no documented operational need that directly supports implementation of wireless network technology, and the USAF has published no Wireless Network CONOPS or associated doctrine.

This is not to say the USAF has done nothing to transform the force and rectify the situation with networks. In accordance with Congressional mandates and out of necessity, the USAF has made numerous organizational adjustments over the years to provide structure, additional oversight and accountability of IT capital expenditures and management. However, the preponderance of these changes were implemented solely to establish institutional fiscal responsibilities and provide improved transparency with respect to network and IT acquisitions, not to address strategic Air Force-wide network-related organizational construct and procedural challenges.

While the USAF likely has all the right functional pieces and skilled personnel to develop the required network CONOPS, doctrine and TTPs, it lacks the organizational structure and operational discipline to harness these assets and maximize their utility. More specifically, unlike other weapon systems, the USAF has yet to establish a strategic centralized authority responsible for all Air Force networks.

In addition to the need for a central authority, the USAF also needs to reorganize at the operational and tactical levels in order to better focus and synchronize the efforts of various, often competing, entities to create synergy and realize the full potential of their combined organizational parts. According to Air Force Basic Doctrine, "centralized control and decentralized execution of air and space forces are critical to force effectiveness."[3] Absent this unity of command, there is no unity of effort and operational synergy is stymied. Although incremental organizational changes have been made in the past to address emerging network-related challenges, most have been aimed at treating base-level symptoms rather than addressing the root cause—the need for a centralized authority and chain of command responsible for the generation of comprehensive integrated network doctrine, CONOPS and TTPs.

Organizational changes of this magnitude cannot occur overnight, nor will they be a one-time fix. While we are transforming our organizational construct and processes, circumstances and technology will continue to evolve, and we will continually need to update and refine our organizational structure and concepts accordingly. But with an integrated, long-term organizational commitment focused on operational needs, we will be better able to make the right decisions to improve warfighting capabilities. The bottom line is that the Air Force can ill afford to continue operating disparate units that lack disciplined synchronization and a common operational vision. The USAF is growing more and more operationally dependent on networks

[3] *Air Force Doctrine Document 1,* Air Force Basic Doctrine, p. 23.

every day, and until a centralized organizational construct is implemented to direct and enforce institutional change, we will continue to experience the same inefficiencies and operational challenges we face today. This analysis provides some historical insight into the network revolution and prescribes a time-proven approach for making the organizational changes necessary to support networks as legitimate weapon systems.

Chapter 2

Background

Over the past three and a half decades, the ability of the DoD to keep pace, operationally as well as organizationally, with advancements in computer and network technologies has proven to be extremely challenging, if not impossible at times. According to Colonel David Gruber, former Director of Air Force Networks, an important aspect of the network revolution within the USAF, which clearly contributed to the organizational challenges we are currently facing, is the fact that it was not preceded by any significant planning.[4] In 1969, the Defense Advanced Research Project Agency designed and implemented a communications network, better known as the ARPANET, which linked several universities and defense facilities into a network that was designed to survive a nuclear blast, identify segments of the network that no longer existed and route traffic around them.[5] Although the ARPANET was initially very limited in scope, according to most historical references it quickly became the preferred method of data communications by the DoD and served as the genesis of modern networks.

In light of its tremendous success, the ARPANET soon became saturated, which led to rapid expansion and the addition of numerous sites.[6] In time, the DoD broke the military portion away from the ARPANET to create the MILNET, which was initially an unclassified communications

[4] David J. Gruber, Lt Col, USAF, *Computer Networks and Information Warfare: Implications for Military Operations*, (Occasional Paper No. 17, Center for Strategy and Technology, Air War College, Air University, Maxwell AFB, AL, July 2000), p. 8.

[5] Bassam Halabi, *Internet Routing Architectures* (Indianapolis, IN: Cisco Press, New Riders Publishing, 1997), p. 3.

[6] Gruber, *Computer Networks and Information Warfare*,,8.

network managed by the Defense Communications Agency (DCA).[7] The National Science Foundation employed lessons learned from the ARPANET effort to create the NSFNET, which was dismantled in 1995 and replaced by today's commercial Internet.

As the MILNET and the Internet evolved and matured, the DoD changed the name of the MILNET to the Defense Data Network (DDN) and expanded it to include other portions of the Internet and classified military networks which were not considered part of the Internet. The DDN was primarily used to connect military installations and was managed by DCA. The DDN was later renamed to what we now know as the Defense Information Switched Network (DISN). During this same period, DCA also changed its name to the Defense Information Systems Agency (DISA). Colonel Gruber stressed the fact that both the civilian and military networks remained compatible during development because they collaborated and intentionally followed common standards.[8]

As networking and computing technologies advanced, both the Internet and the DISN were continually expanded and refined. Formal committees were created, first by the Government and then by industry and concerned users, to develop, evaluate and approve new ideas.[9] Although network technology matured rapidly and significantly improved capabilities, Colonel Gruber observed that the DISN and the Internet lacked central oversight, system-wide management capabilities and built-in security, all of which hindered the DoD, industry and universities when they tried to connect equipment from various manufacturers.[10] It became apparent that the

[7] Douglas E. Comer, *Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition,* (Upper Saddle River, New Jersey: Prentice Hall, 1995), p. 37.

[8] Gruber, *Computer Networks and Information Warfare,*8.

[9] Ibid.,8.

[10] Ibid.,8.

growth of the DISN and the Internet would require centralized control and strong network management, which led to the establishment of the Institute of Electrical and Electronics Engineers and a series of new protocols.[11] In just a few short years, the DoD expanded the DISN to include nearly every military base, but crafted no formal strategic vision for its future operational use.[12] Similarly, the Air Force established no centralized controlling authority to oversee Air Force networks.

[11] Marshall T. Rose, *The Simple Book: An Introduction to Management of TCP/IP based internets*, (Englewood Cliffs, New Jersey: Prentice Hall, 1991), p. xx.

[12] Gruber, *Computer Networks and Information Warfare,*8.

Chapter 3

Growing Pains

In the early 1980s, the USAF began to understand, appreciate and apply the power of personal computers. In 1981, Air Force Communications Command (AFCC) created an office automation system, which within three years had grown into a local network that linked more than 600 computers.[13] This new capability quickly led to the automation of a number of office tasks and processes such as scheduling, suspense tracking, file sharing and storage, and electronic mail (e-mail). As a result of this success, AFCC, now the Air Force Communications Agency (AFCA), established a Local Area Network (LAN) Office, which it tasked to develop standards for the rest of the Air Force.[14] However, as Colonel Gruber aptly points out, AFCC lacked the authority to make its recommended standards mandatory or to enforce them across the Air Force.[15] Unfortunately, both of these challenges persist to some extent even today.

The fact that networking and computing power have doubled approximately every eighteen months or less since the late 1970s, in what is now known as Moore's Law, had a significant impact on the USAF and the evolution of Air Force networks. In 1979, Intel Corporation co-founder Gordon Moore noted that the density of transistors on integrated computer chips, and thus the price-to-performance ratio of computers, doubled every eighteen months, which he predicted would continue for at least another two decades.[16] As computers became more capable and less expensive, the USAF established standard "Desktop" contracts and blanket purchase

[13] http://public.afca.af.mil/history_pages/flares_to_satellites.pdf, p. 50.
[14] Gruber, *Computer Networks and Information Warfare,*10.
[15] Ibid., 10.
[16] George Gilder, "The Bandwidth Tidal Wave," *Forbes ASAP*, December 5, 1994, http://www.seas.upenn.edu/~gaj1/bandgg.html

agreements that permitted any Air Force organization to buy them.[17] Once organizations were granted the authority to procure their own computers and connect them as they saw fit, bases built LANs that allowed units to share applications, forms, calendars, files, printers and much more.[18] Colonel Gruber observed that the problem with this 'ungoverned' activity was that most squadron LANs were designed and installed in an ad hoc fashion by inexperienced people who did not have well-defined technical standards and maintenance concepts to follow, the skilled personnel to operate them or adequate funding for sustainment.[19] In some cases, Colonel Gruber asserted these "home grown" networks proved so unreliable and labor intensive that they undermined the very efficiency the squadrons had hoped to gain by their use.[20]

The "e-mail explosion" of the mid 1990s, which began as a convenient way to communicate, quickly became the primary means for transferring information and proved to be a significant event in the evolution of networks. The Air Staff soon began to rely heavily on e-mail as the "unofficial," yet most efficient, means of getting their message out to the field.[21] Local base leadership quickly learned that the loss of important e-mail messages could have severe organizational and operational repercussions.[22] Soon wing commanders began directing their communications personnel to connect these disparate squadron LANs, and by 1994 nearly all wing, group and squadron commanders had e-mail capability at their fingertips.[23] However, the Air Force quickly realized that the level of responsibility required to operate and maintain these kludged networks could not be adequately managed given the fact that most, if not all, initial

[17] Gruber, *Computer Networks and Information Warfare*,10.
[18] Ibid., 10.
[19] Ibid.,11.
[20] Ibid.,11.
[21] Ibid., 11.
[22] Ibid., 11.
[23] Ibid., 11.

base network infrastructures were poorly designed, adhering to no industry or DoD standards, under-funded and maintained by untrained communications technicians.[24]

Once Air Force leadership recognized that their operational and administrative dependence on networks and the base information infrastructure was growing, they quickly began to reorganize and develop policies and guidance for managing the systems.[25] For example, the Air Force created Network Control Centers (NCC) with responsibility for all of the base's networks as well as all data and information that entered and left the base.[26] The Air Force fielded standard automated network management tools, assigned personnel from the communications squadron to work in the NCCs and established a formal network technician training schoolhouse and standards, all of which were essential steps in establishing some measure of operational discipline and rigor. Although not specifically authorized, other organizations and functional communities on USAF bases continued to procure equipment and create their own LANs.[27] While the NCC was theoretically responsible for network growth, in practical terms any organization that had funds to spend on communications and/or computer equipment could add what they wanted, and did so with relative impunity.[28]

After enduring several years of growing pains, Air Force leadership finally assigned the NCC responsibility to centrally manage base network growth. This decision formally signified that networks were critical to the success of military operations and was the prelude to networks being declared weapon systems. If the network went down for any reason, people at the base

[24] Gruber, *Computer Networks and Information Warfare*, 11.
[25] Ibid., 11.
[26] Ibid., 11.
[27] Ibid., 11.
[28] Ibid., 11.

would not be able to conduct business as usual and many critical processes would come to a complete halt.[29]

Another challenge that Colonel Gruber cited was that organizations which had dedicated their own manpower to operate their respective functional LANs were often reluctant to give control of the LAN to the NCC.[30] As a result of leadership's failure to plan for and allocate additional manpower to support the LANs, the NCCs could not immediately guarantee that they could provide the same level of service as the organizations previously enjoyed.[31] Not surprisingly, it was not uncommon for functional communities that could spare the manpower to establish "fiefdoms" or rogue networks on the base, which they owned but were in fact controlled by the NCC.[32]

As the struggle for control of the networks among base-level functional communities and the NCCs came to an end with Air Staff assigning the NCCs authority and control of all base-level networks, Air Force leadership realized there was still no institutional controlling authority or coherent glide path for networks. More importantly, the Air Force realized base-level networks were no longer "islands in the stream," but rather interconnected components of the much larger DISN with operational interdependencies, shared responsibilities and shared vulnerabilities. To some extent, base NCCs had become "sanctioned" fiefdoms, answering only to the base commander and local leadership. This realization of network interdependence in turn drove the Air Force to establish two new organizations within the network hierarchy at the MAJCOM and Air Force levels, the Network Operations and Security Centers (NOSC) and the Air Force Network Operations and Security Center (AFNOSC). (See figure 3-1).

[29] Gruber, *Computer Networks and Information Warfare*,12.
[30] Ibid., 12.
[31] Ibid., 12.
[32] Ibid., 12.

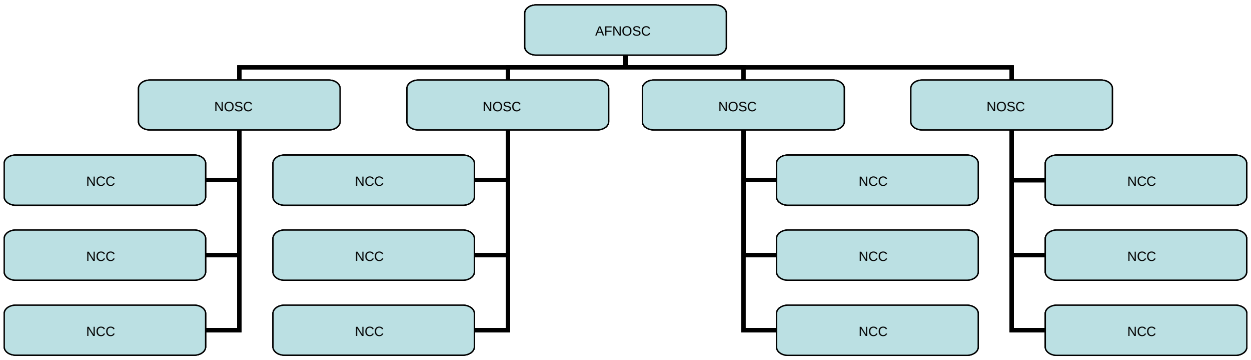

Figure 3-1. Air Force Network Organizational Hierarchy as proposed in 1998

In keeping with the basic tenets of airpower, centralized control and decentralized execution, ACC created and implemented the NOSC in the late 1990s to provide COMACC centralized control over all ACC base-level networks and to provide shared network situational awareness across the command, while NCCs continued performing the decentralized operations. The NOSC construct was an immediate success and was quickly adopted and implemented by all the MAJCOMs.

The organizational construct proposed by ACC also called for the creation of an AFNOSC at the Air Force level to provide centralized control and oversight of network operations Air Force wide. While this concept was readily accepted by the Air Staff, leadership could not decide who should become the central authority or commander of the AFNOSC and more importantly, where this organization would fit within the Air Force hierarchy. Regretfully, only the operations and reporting portions of the original AFNOSC construct were initially implemented, leaving out the all-important requirement to establish a central command authority.

Only now, some seven years later, is the Air Force finally attempting to fill this central control void by establishing the recently proposed AFNetOps Command under the Eighth Air Force Commander. While the current notional organization (Figure 3-2) establishes a bona fide central operational authority and operational units, it appears to ignore the basic needs for CONOPS and doctrine development. Until the Air Force establishes organizations with formal responsibilities for the development of network weapon systems CONOPS and doctrine, it is likely this AFNetOps effort will fall short of the mark as well. Only time will tell whether or not the AFNetOps organization will in fact provide the centralized authority and advocacy Air Force network weapon systems currently lack, but so desperately need.

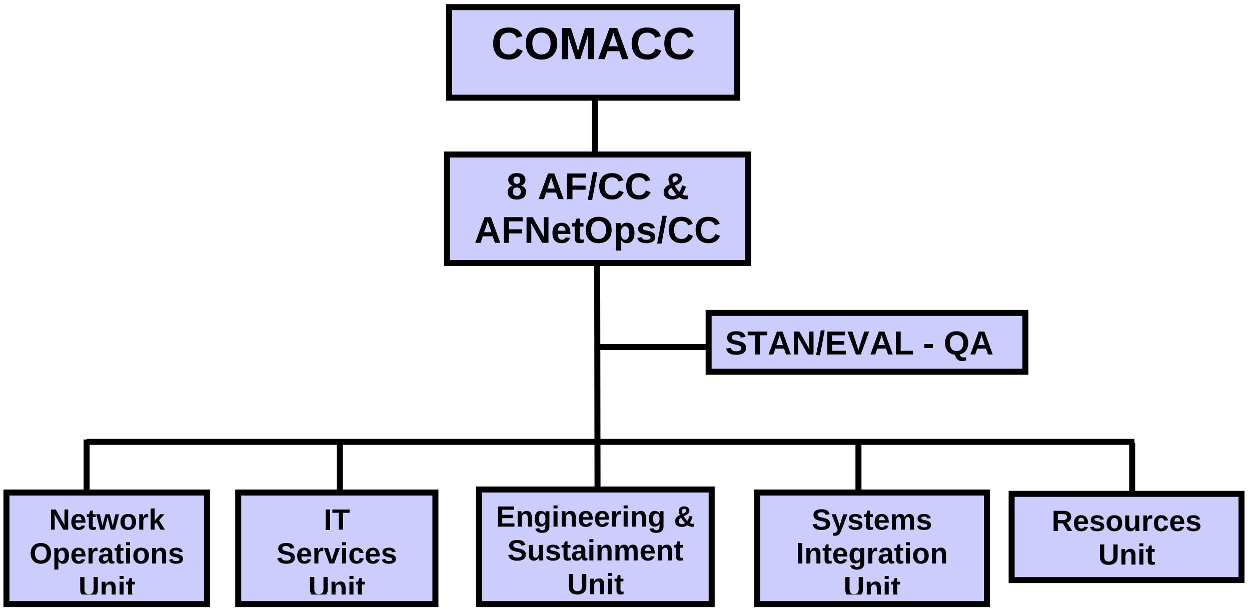

Figure 3-2 Notional AFNetOps Organization

While the creation of the AFNetOps Command is the latest in a long line of internal Air Force organizational initiatives aimed at legitimizing networks as bona fide operational weapon systems, external agencies have also influenced Air Force organizations but with non-operational objectives in mind. The most notable external influences resulted from new laws and reform acts established by the U.S. Congress, most of which were designed to promoted accountability and improve transparency of DoD IT acquisitions. In addition to achieving their stated goals, these Congressional mandates also created new leadership roles and responsibilities which in turn spawned new organizational constructs across the DoD.

Chapter 4

External Influence

As network technologies continued to mature, the USAF sought to enhance productivity through automation, but there were many failures.[33] According to Colonel Gruber, the challenge typically encountered by a systems program office (SPO) was that the incremental expansion of system requirements led to automating too many functions simultaneously.[34] Usually, it took only a few minor requirement “add-ons” before the system became so complex that doubts about whether it could actually be developed successfully would surface.[35] He stressed that this “requirements creep” was not the only reason for failure.[36] In some cases, Colonel Gruber claimed the concepts were too advanced and the requirements were simply too complex for current technology.[37] Failures in several major programs eventually caused the DoD to restrict the growth of military requirements and forced the military services to better estimate the total lifecycle costs of IT projects.[38] Additionally, in response to the challenges of the government spending billions of dollars on IT systems that often failed to produce anticipated results, Congress passed the Information Technology Management Reform Act, often referred to as the

[33] Gruber, *Computer Networks and Information Warfare,*13.
[34] Ibid., 13.
[35] Ibid., 13.
[36] Ibid., 13.
[37] Ibid., 13.
[38] In a report to Congress in 1995, the GSA stated that the “Estimated development costs can skyrocket due to poorly defined or shifting requirements. Delays in developing and deploying a new system can erode projected benefits and delay returns on investment, and poorly designed systems can aggravate operational problems or create new ones. In the worst cases, systems development efforts can suffer from a cascade of problems that lead to the termination of the efforts and a total waste of funding. Large "grand design" systems are particularly vulnerable to such problems because of their "all or nothing" approach. Information Technology Investment: A Government wide Overview (Letter Report, 07/31/95, GAO/AIMD-95-208). Letter from the Government Accounting Office to the Chairman, Committee on Governmental Affairs, U.S. Senate, July 1995. Found at URL http://www.gao.gov/archive/1995/ai95208.pdf. p. 10

Clinger-Cohen Act, after its sponsors Senator William Cohen and Representative William Clinger.

The primary intent of the Clinger-Cohen Act sought to "streamline IT acquisitions and emphasize lifecycle management of IT as a capital investment," and significantly altered how the government developed, procured, and operated IT.[39] Instead of centralizing federal IT acquisition under one organization, which the Brooks Act previously established, it gave the Office of Management and Budget overall responsibility for acquisition and management policy, and made the heads of executive agencies responsible for acquiring IT and effectively managing their technology investments.[40] Colonel Gruber touted the Clinger-Cohen Act as a landmark piece of legislation because it mandated accountability of federal agencies and departments, requiring them to demonstrate that investments in IT would actually improve business processes.[41] In essence, "Congress wanted evidence that the money being invested in IT would result in cost savings and increased efficiency."[42]

Under this Act, the services were given full, independent acquisition authority for their respective IT investments.[43] The Act also required executive agencies to appoint a Chief Information Officer (CIO), which in addition to advising the head of the executive agency, would be responsible for developing, maintaining, and implementing the organization's IT

[39] Robert Lagas, *Information Technology Management Reform Act Summary* (Office of Information Resources Management, National Institute of Health), http://www.icesa.org/articles/template.cfm?results_art_filename=itmrasum.htm

[40] *Information Technology Management Reform Act (ITMRA) of 1995*, Public Law, SEC. 5121-5124, http://irm.cit.nih.gov/itmra/itmra96.html

[41] Gruber, *Computer Networks and Information Warfare*,14.

[42] Ibid., 14.

[43] http://public.afca.af.mil/history_pages/flares_to_satellites.pdf, p. 71.

architecture as well as automating work processes.[44] The primary objectives were for the CIO to manage the network equipment, computers and software applications and improve the acquisition and use of IT in support of the Air Force mission.

As intended, the Clinger-Cohen Act successfully served as an organizational change agent for the DoD. In the Air Force, the Assistant Secretary of the Air Force for Acquisition was appointed as the first Air Force CIO, and in this capacity worked directly for the Secretary of the Air Force. The Air Force CIO had the authority to delegate its power to subordinate commands, which in turn allowed the Air Force MAJCOMs to appoint their own directors of command, control, and communications, who reported to both their respective MAJCOM commander as well as the Air Force CIO.[45]

It was under this new construct that the USAF secured the means to resolve a number of challenges.[46] A prime example offered by Colonel Gruber was the newfound ability to apply some measure of oversight and standardization to the increasing number of automated systems that in the past were created in a "stovepipe" fashion.[47] He argued that while finance officials developed finance systems, the medical community developed medical systems and intelligence agencies developed intelligence systems, there was no central authority to ensure that the systems and applications were optimized to support the needs of users or that they were interoperable.[48] Moreover, no one was charged with the responsibility to analyze the traffic or security implications of these disparate systems and applications for the Air Force.[49] The Clinger-Cohen Act presented an opportunity to address these challenges at the operational level

[44] *ITMRA of 1995,* Public Law, SEC. 5123, http://irm.cit.nih.gov/itmra/itmra96.html
[45] Gruber, *Computer Networks and Information Warfare,*14..
[46] Ibid., 14.
[47] Ibid., 14.
[48] Ibid., 14.
[49] Ibid., 14.

because, for the first time, CIOs were given the authority to integrate IT projects across the DoD, the Air Force and the major commands.[50] This development would have profound implications for the USAF as it shifted toward an expeditionary force and a new net-centric organizational and operational construct in the late 1990s.[51] While the Clinger-Cohen Act accomplished its objectives and moved the Air Force in the right organizational direction, it too fell short of establishing true centralized control at the strategic level.

In essence, networks grew from useful tools for sharing printers and files to weapon systems that determined the ability of the USAF to accomplish its peacetime and wartime missions.[52] The USAF has made efforts to incorporate emerging network capabilities in the name of efficiency and mission accomplishment, and has assigned responsibility and accountability at the operational and tactical levels, all necessary and important steps. However, as an institution, it has consistently failed to recognize the need to establish a strategic centralized authority and the supporting organizational structure necessary to leverage existing forces and truly transform today’s networks into legitimate comprehensive, integrated weapon systems.

[50] Gruber, *Computer Networks and Information Warfare,*15.
[51] Ibid., 15.
[52] Ibid., 12.

Chapter 5

Presentation of Forces

There are three prominent organizations within the USAF which collectively possess the equipment, contract vehicles and skilled personnel capable of developing network CONOPS, doctrine, TTPs and much more. Unfortunately, AFCA, which reports to Air Staff; the Air Force Information Warfare Center (AFIWC), which reports to ACC; and the Electronic Systems Center (ESC), which reports to AFMC, all fall under different command authorities and therefore share no formal organizational linkage. In the absence of unity of command or centralized control, these organizations are left to their own devices and allowed to pursue their own agendas, which has in turn led to poor coordination, duplication of effort, operational gaps and seams and overall inefficiency. From an organizational standpoint, this translates into very little or no unity of effort when it comes to network weapon systems.

These three organizations are depicted in the Venn diagram at Figure 5-1 below, denoting their respective core competencies, and highlighting duplication of effort and operational gaps and seams. For example, all three organizations develop network TTPs to some degree; they all generate, solicit and validate requirements; they all perform or support network design and engineering; they all perform acquisition-related functions; two of the three possess emergency network response teams; they all perform network analysis; and all three conduct R&D programs to some extent. More important is the fact that none of these organizations are responsible to develop Air Force network doctrine or CONOPS, only AFCA generates network policy, and AFIWC possesses the Air Force's only Network Red Team assets.

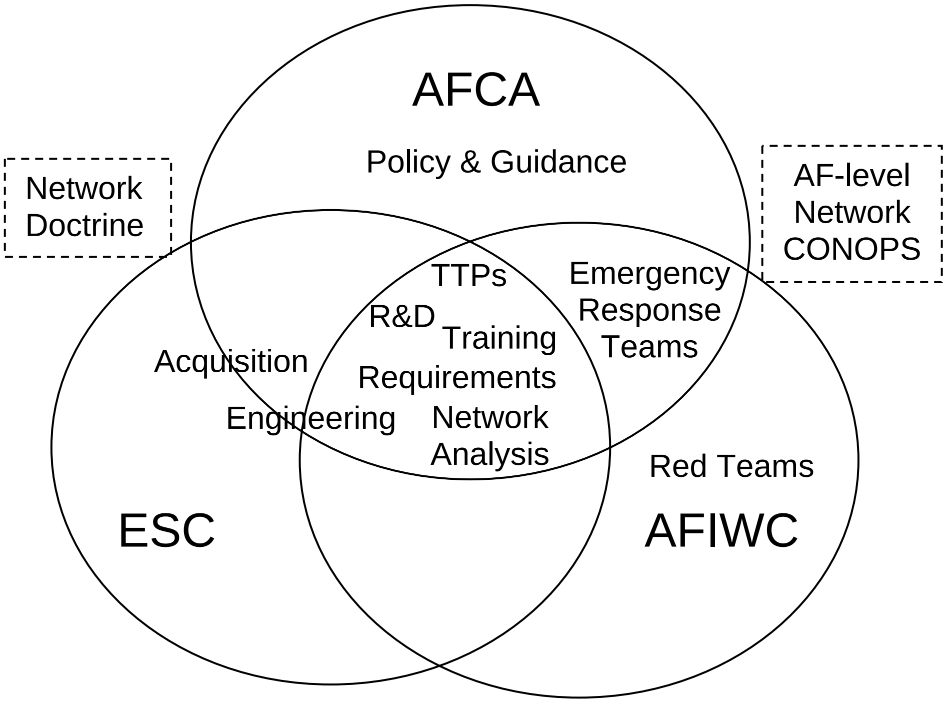

Figure 5-1. Organizational Core Competencies

Not displayed in the figure is the disjointedness and lack of cohesion among these organizations, which can also be attributed to the lack of any formal centralized network control authority to coordinate efforts, deconflict schedules and synchronize processes. The intent of this organizational comparison is simply to show that each of these organizations perform functions and possess legitimate core competencies that the Air Force can leverage to support a new organizational construct and operate more efficiently. In order to realize these operational and fiscal benefits, it is critical that AFCA, AFIWC and ESC work together collaboratively, not competitively, toward common goals and objectives. Therefore, the challenge facing leadership lies in determining which of these organization(s) is/are best suited to perform each of the specified functions, assigning roles and responsibility, and divesting of duplicative, inefficient resources and processes. Although AFCA, AFIWC and ESC were originally created to perform complementary functions, there was no central authority to keep them in check and prevent mission creep from occurring. Hence, we have all three performing some required activities, and no one performing others.

Air Force Communications Agency

The Agency is a field operating agency that reports directly to Headquarters USAF and its primary mission is to support air and space operations by bringing expertise in the communications and information arena to the fight. Additionally, AFCA is responsible to advocate for USAF-wide communications and information planning, resourcing, testing, training, implementation and sustainment. Headquartered at Scott AFB, IL, AFCA has a history of innovation, but a reputation among commanders in the field for being out-of-touch with operational requirements, late-to-need with capabilities and policy, and a bit self-serving.

Specifically, AFCA is chartered to "direct the integration of systems onto the Air Force network to achieve integrated and interoperable Air Force concepts of operation capabilities."[53] So to some extent, AFCA is already in the CONOPS business at the operational level, but not at the strategic level. The overarching objective is to provide seamless connectivity for the command and control of air and space forces. Although AFCA drives innovative solutions for the warfighter by generating progressive standards, architectures and force structure policies and guidance, they have often failed to vet their products through other highly skilled and specialized Air Force organizations—like AFIWC—prior to acquisition and fielding. A classic example occurred in 2001 when AFCA developed and fielded a software patch that was intended to make the Defense Message System fully compatible with the commercial version of Microsoft Exchange. In their haste, and against the objection of field units, AFCA direct NCCs to

[53] AFCA web site, https://private.afca.af.mil/

implement the patch prior to the completion of objective testing, subsequently breaking nearly every official and commercial messaging capability across the Air Force for several weeks.

One of the stated primary objectives of the Agency is to "drive innovation for information superiority by exploiting and certifying new technologies and systems Air Force wide."[54] In this capacity, the Agency also serves as communications force structure and policy experts, but has not taken on the formal responsibility for developing service-level network doctrine. As the USAF's lead agency for network guidance and policy, it seems only logical that AFCA is best postured to take on the responsibility to generate service-level doctrine and CONOPS as well.

As an aside, "AFCA leads the Air Force in information infrastructure optimization and deploying rapid response command, control, communications, and computer (C4) strike teams world-wide for assured Air Force network combat power."[55] Perhaps if Air Force networks were designed better prior to fielding, fully employing the special skills resident within AFIWC and other organizations, there would be little need for strike teams.

Air Force Information Warfare Center

Activated on Sept. 10, 1993, the Air Force Information Warfare Center (AFIWC) is not only the focal point for development and application of information dominance in future warfare, but it also provides commanders with products and services to wage command and control warfare.[56] The Center is also charged with protecting friendly command and control capability including USAF computer security. It is the primary source of electronic warfare and command, control and communications countermeasure analysis and advice for the Air Force.

[54] AFCA web site, https://private.afca.af.mil/
[55] AFCA web site, https://private.afca.af.mil/
[56] Air Force Information Warfare Center (AFIWC) Mission Brief, "Delivering IO Combat Power."

The AFIWC performs network and systems analyses to support planning, developing and testing using the latest network and electronic warfare equipment. The Center also supports the network and electronic combat acquisition process, from development of statements of need through final testing by providing specialized analysis to USAF MAJCOMs and the Air Staff. These specialized functions, coupled with the network Red Teams or Aggressor units, make AFIWC uniquely qualified to perform functions critical to network design and security. Perhaps most disconcerting is the continued reluctance of Air Force leadership to fully utilize AFIWC Red Teams. To date, the Air Force has not instituted a formal process to capitalize on AFIWC's specialized capabilities and incorporate Red Team findings and lessons learned into doctrine, TTPs and Air Force-wide network policies.

The Center is often called upon by AFCA and MAJCOMs to orchestrate and support real-world operations planning and exercises, and is uniquely postured to help assess network products for performance, vulnerabilities and survivability. However, current network SPO acquisition activities typically begin with out sourcing these product assessments to integrating contractors, largely ignoring AFIWC. In essence, multiple contractors are given systems requirements and tasked to develop engineering designs comprised exclusively of commercial off-the-shelf (COTS) IT components.[57] According to Colonel David Nicholls, the Vice Commander of AFIWC, while COTS products are typically easy to use and readily available, they are often times not the best solution.[58] Hence, AFIWC also maintains the capability to engineer sensitive network security, intrusion detection and performance management components and applications in house. As Colonel Nicholls puts it, we simply cannot entrust the

[57] Sanders, CITS Briefing

[58] Colonel David J. Nicholls (Vice Commander, Air Force Information Warfare Center), interview with the author, 18 November 2005

security of our networks and information to software code and technologies that are available to anyone and everyone who can afford to purchase them—this would equate to an open invitation for network exploitation.[59] The bottom line is that current Air Force processes fail to leverage and/or fully integrate the unique capabilities AFIWC brings to the fight.

Electronic Systems Center

Air Force Materiel Command's Electronic Systems Center (ESC) manages the development and acquisition of electronic command, and control, (C2) systems, but doesn't actually design or manufacture equipment; they hire civilian contractors to do that. In its systems acquisition mission, ESC serves as the manager. It determines the operational user's needs, defines systems to best meet those needs, ask for proposals from industry, selects contractors and monitors their progress. Teams of professionals specializing in engineering science, business management, acquisition and computers supervise the design, development, testing, production and deployment of C2 systems.[60]

According to their mission documents, "the ESC is the Air Force's center of excellence for the development, fielding and sustaining of command, control, intelligence, surveillance, reconnaissance and combat support systems."[61] As shown in Table 5-1, many of the very same functions ESC pays contractors to perform are also being performed by AFCA and AFIWC. The Center's stated mission is to deliver the power of information to the warfighter. To accomplish this mission, the Center's efforts are justifiably focused on many of the same areas as AFCA and AFIWC, and to some extent all three organizations are operating in vacuums sans any unity of command, collaboration or coordination.

[59] Colonel David J. Nicholls (Vice Commander, Air Force Information Warfare Center), interview by the author, 18 November 2005

[60] ESC home page, http://esc.hanscom.af.mil/default.asp

[61] ESC home page, http://esc.hanscom.af.mil/default.asp

The bottom line is, the USAF has multiple, often competing, organizations performing similar, if not redundant functions. Absent are unity of command, a shared strategic transformation vision and the associated framework for collaboration and convergence of these entities. As with other weapon systems, the USAF needs to develop and maintain strategic CONOPS and doctrine for networks, synchronizing key design and procurement milestones among the various organizations, thereby providing a means to ensure emerging operational mission sets are being addressed at the right time, by the right agency and aligned with the intent of the DoD strategic plan.

In addition, as the Air Force continues to downsize and the budget continues to shrink, it is important that the new construct help the USAF reprioritize and divest of non-critical legacy workload to free-up resources to support new mission requirements as they emerge. Last, the construct must provide a feedback mechanism to ensure lessons learned are captured and incorporated appropriately to produce consistent network design, enhanced security, timely TTPs, relevant inspection criteria and doctrine.

The question is, what organizational construct or model should the Air Force employ and why? While there are various schools of thought on how best to reorganize, perhaps the best place to start is by examining the processes and organizational constructs currently in use by other well-established weapon systems. The key is not to throw the baby out with the bath water. In essence, AFCA, AFIWC and ESC are all postured to make meaningful contributions to the advancement of network weapon systems and the Air Force should not completely divest of these organizations and their capabilities. Rather the Air Force should seek to apply a proven organizational model to better integrate and synchronize the efforts of these organizations, capitalizing on the key attributes and core competencies of each.

Chapter 6

A Framework for Success—The Road Ahead

The organizational and operational challenges the USAF faces today with respect to development of doctrine, CONOPS and TTPs to support network weapon systems are not new nor are they unique to the communications and information community. In many respects, they are the very same challenges Tactical Air Command (TAC) and Strategic Air Command (SAC), which in 1992 merged combat forces under Air Combat Command (ACC), encountered decades ago with aircraft weapon systems and have since overcome. Success for the flying community resulted in part from strict adherence to the tenets of Airpower, centralized control and decentralized execution, and basic Air Force doctrine. First and foremost, by establishing the Commanders of TAC and SAC, typically the most senior and influential four-star generals in the USAF, the commands' anointed formal "top customers" and established all important centralized control.

The establishment of a principal operational advocate or "top customer" to take on Air Force-wide network issues must be a top priority. In an effort to fill this void, the AFNetOps Command is being designed to centralize the command and reporting structure, while consolidating dispersed functions, personnel and resources in the areas of network operations, architectures and analysis, network defense, policy, information technology services, TTPs, acquisition and sustainment. The benefits of this construct include unified and improved C2 capabilities, directive authority to ensure operational compliance and standardized operations across the Air Force.

If the AFNetOps construct is successfully implemented, the network weapon systems could soon begin to realize the operational benefits and level of influence currently afforded to other functional communities. For example, when the Combat Air Forces (CAF) suffers design- or parts-related Class A mishaps, the ACC Commander as the CAF lead is postured to influence the responsible parties to initiate fix actions immediately. While the communications community has attempted to model network mishap and other operational command and reporting processes after those successfully employed within the flying community, the absence of a central authority figure has rendered many efforts impotent—failing to gain the traction or garner the operational support and resources required to succeed.

The establishment of the new AFNetOps Commander as the "top customer" for USAF network operations is clearly a step in the right direction, but there are still other areas that require attention. This chapter compares and contrasts the communications and flying communities, highlighting some opportunities to apply well-vetted organizational constructs and processes employed by the CAF to the challenges the USAF is currently facing with respect to network weapon systems. Specifically, this framework focuses on three main tenets--doctrine, CONOPS, and TTPs.

The first tenet that is clearly missing from the network organizational construct is the assigned responsibility to develop service-level network doctrine. Noted authors on doctrine and military strategy, Dennis Drew and Don Snow defined military doctrine "as what we believe about the best way to conduct military affairs."[62] Therefore, by definition, doctrine is intended to serve as a guide for how best to organize, present, deploy and employ forces and resources.

[62] *Making Strategy: An Introduction to National Security Processes and Problems*, Chapter 11, August 1988, pp. 163–174. Published 1988 by Air University Press.

Consequently, in the absence of any true official network doctrine, it is difficult to answer the big questions pertaining to proper mission sets, organizational constructs, control, resources and support. According to basic USAF doctrine, two of the guiding principles that are key pillars to operational success are unity of command and centralized control coupled with decentralized execution.[63] The flying community has embraced and institutionalized both of these principles, while the communications community has not. Many on the Air Staff seem to think the new AFNetOps organization, under the command of the Eighth Air Force Commander, will fill the unity of command or centralized control void.[64] However, the Air Force still needs the operational discipline and supporting doctrine to realize true decentralized execution under this construct.

As discussed in previous chapters, the Air Force Communications Agency's charter is to develop policy and guidance for Air Force networks.[65] And, since policy typically sets the boundaries for doctrine and strategy, it logically follows AFCA is best suited to shoulder the responsibility for developing Air Force networks doctrine. But there is no need to start at ground zero, as the Air Force already has a well established construct and process for doctrine development. In fact, leadership at the Air Force Doctrine Center recommends AFCA simply get on board with the rest of the Air Force and synchronize its efforts with the existing service doctrine development cycle.[66]

The second tenet centers on the USAF's inability to learn from our mistakes and the mistakes of others in developing actionable network TTPs as an adjunct to formal doctrine.

[63] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003, pp. ix.
[64] Air Staff XCI Briefing to SAF/XC-2, *Air Force NetOps Transformation: Integrated Network Operations and Security Center (I-NOSC)*, 6 July 2005

[65] AFCA web site, https://private.afca.af.mil/
[66] Colonel Kent Williams (Deputy Director, Air Force Doctrine Center), in discussion with author, 30 November 2005

Again, the similarities among the flying community and the communications community are striking, yet these similarities go largely unnoticed or are simply ignored. In the CAF for instance, we have the USAF Warfare Center, headquartered at Nellis AFB, which manages advanced pilot training and integrates many of the Air Force's test and evaluation requirements into operational TTPs and the formal doctrine process. Established in 1966, the Center has had nearly 40 years to concentrate on the development and refinement of forces and weapons systems that are specifically geared to air operations in war and contingencies.[67] A clear parallel can be drawn comparing the functions performed by USAF Warfare Center to those performed by the AFIWC. Both organizations possess vast test ranges (real and virtual), Red Teams or aggressor units, conduct tests, evaluations and exercises, perform training, develop, test and validate TTPs, and influence doctrine and weapon system safety, security and operational capabilities. Instead of starting from scratch, the USAF would be well served to emulate the proven processes the USAF Warfare Center has refined over the past four decades.

Specifically, the USAF Warfare Center conducts Red Flag exercises several times each year to afford Airmen the opportunity to practice employment tactics throughout the full spectrum of tactical warfare (i.e. practice the way we plan to fight). These exercises are designed to enhance flying safety, replicate viable and current threats, target arrays, and C2 architectures in scenarios that simulate wartime flying operations, generate and disseminate lessons learned, promote the free exchange and employment of tactical ideas, and introduce aircrews to enablers that are critical to the success of tactical warfare.[68]

[67] Nellis Air Force Base web site, http://www.nellis.af.mil/units.htm
[68] Nellis AFB web site, http://www.nellis.af.mil/units.htm

Similarly, the AFIWC has employed Red Teams or aggressor squads to conduct network vulnerability assessments for years. Unfortunately, these assessments are not performed as part of a holistic Air Force-wide strategy to assess and remediate network vulnerabilities and enhance security. In fact, the results of these assessments or lessons learned are typically not used to resolve Air Force-wide challenges, develop actionable TTPs, enhance network design or influence training and inspection criteria. Instead, since the assessments are primarily conducted at the behest of local command authorities, the results and lessons learned are kept close-hold and released only to the requesting commander for local use. In the absence of any formal or informal cross-feed mechanism, it is therefore not surprising that the Red Teams consistently find many, if not all, of the same vulnerabilities at nearly every base they visit.

The CAF employs a more holistic strategic construct to capture and synthesize lessons learned from Red Flag exercises and real-world operations to develop new TTPs and influence doctrine. The absence of any such formal strategic process is only now being recognized and addressed in the network arena. Recently, the USAF has taken positive steps to emulate Red Flag by conducting network exercises like Black Demon 2005 and is in the process of using the results to affect systemic change through the development of new TTPs and enhanced training.

The USAF Warfare Center and AFIWC have other attributes and capabilities in common. Specifically, the USAF Warfare Center mission also encompasses the USAF Weapons School for training, the USAF Air Demonstration Squadron (Thunderbirds) and several prominent test and evaluation organizations.[69] While the AFIWC does not boast a demonstration team, their ability to perform network training, testing and evaluations is unrivaled. Unfortunately, most of these resources remain largely untapped by the greater USAF and are instead inward focused,

[69] Nellis AFB web site, http://www.nellis.af.mil/units.htm

predominantly serving internal AFIWC and National Intelligence Community requirements. Only recently has the USAF begun to capitalize on these unique resources to test and validate network TTPs for service-wide implementation. Initial indications from Air Staff are that the transformation strategy for the AFNetOps Command will seek to leverage these AFIWC resources to an even greater extent.

The similarities among the two weapon system communities aren't limited to just the USAF Warfare Center and AFIWC. The flying community has SPOs for each respective weapon system, all of which operate under the control of Air Force Materiel Command. Likewise, the USAF's primary SPO for network weapon systems is ESC, which, as mentioned previously, also falls under Air Force Materiel Command. The main difference between the two communities lies in the ability of the flying world's central authority figure, COMACC, to influence SPO activities and drive responsiveness to CAF-wide requirements. If instituted properly, the AFNetOps Command, possibly through COMACC proxy, will likely be able to emulate many of the CAF processes to directly influence network-related activities not only at the SPO level, but across the entire Air Force.

Basically, the Air Force needs to reorganize its network-related functions to establish unity of command and promote unity of effort. The service already has all the key components in its arsenal to produce network doctrine, CONOPS, and TTPs, but absent a central controlling authority to synchronize activities, processes and timelines most efforts have been disjointed and consequently fallen short of the mark. While there are many theories on how best to reorganize these functions, the CAF provides an extremely effective organizational model which is certainly worthy of emulation.

Chapter 7

Conclusion

If the organizational construct and processes the Air Force employed to support network weapon systems were similar to those of the flying community, the focus would shift from allowing three separate organizations to operate independently to ensuring that the efforts of all three are well coordinated and synchronized--in much the same way as the current CAF model functions. Through the application of basic Air Force doctrine to establish centralized control and decentralized execution, network technicians, operators and users alike would all realize profound enhancements in network operations, support, doctrine, CONOPS and TTPs.

The first step of this organizational change should be to establish unity of command for all network weapon systems and lay the foundation for centralized control and decentralized execution. The USAF is currently in the midst of creating this framework under the emerging AFNetOps Command. Establishing unity of command for network weapon systems means the USAF will finally have one principal authority responsible to create a holistic network vision, oversee and coordinate operations, establish common goal and objectives, advocate for funding and sustainment, focus training efforts, direct the development of consistent TTPs and establish network doctrine.[70]

The second step of this Air Force-wide perturbation is the need to realign and synchronize the efforts of AFCA, AFIWC and ESC along a common timeline to produce network CONOPS, optimized network designs, enhanced security, improved training and TTPs and ensure inclusion in the USAF doctrine development cycle. However, this action will also require the Air Force to

[70] Air Staff XCI Briefing to SAF/XC-2, *Air Force NetOps Transformation: Integrated Network Operations and Security Center (I-NOSC)*, 6 July 2005

more clearly define and deconflict the roles and responsibilities of these organizations. While AFCA, AFIWC and ESC all bring vast amounts of experience and some unique capabilities to the table, they also possess many of the same capabilities and perform many of the same functions. Instead of maintaining or contracting redundant skills and capabilities, the USAF needs to determine which organization is best suited to perform each specified activity and label that organization the “center of excellence” for that particular activity. The other organizations will then be able to divest of duplicative capabilities and the associated costs, thereby streamlining the process and improving overall efficiency. This is not to infer that some overlap of activities and/or functions is not warranted and should not continue. For example, it is a reasonable expectation that all three organizations will continue to have a hand in the TTP and requirements identification, development and validation processes. It is also logical and prudent that all three maintain some level of involvement in identifying, developing, refining, facilitating, coordinating and controlling training. The Venn diagram at Figure 7-1 provides a possible strategic realignment construct for consideration.

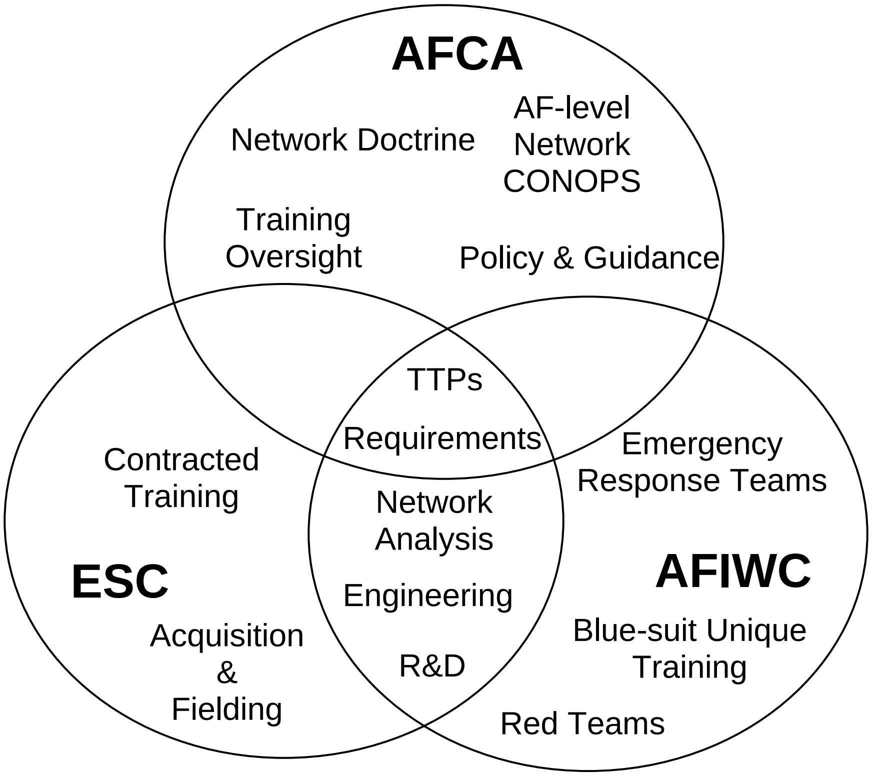

Figure 7-1. Proposed Realignment of Core Competencies

In conclusion, the USAF needs to implement a new organizational construct, possibly modeled after the existing CAF structure, to provide centralized control and decentralized execution for network weapon systems. The ultimate goals of this reorganization are to promote unity of effort, consolidate dispersed functions, personnel and resources, and produce legitimate network doctrine, CONOPS and TTPs. The USAF is presently embarking on a new organizational course by creating the AFNetOps Command, which will almost certainly increase short-term costs and experience challenges, but has the potential to reap tremendous long-term benefits. Continued organizational inefficiencies and operational failures, on the other hand, will be far too expensive for the military and our nation to bear.

It is inevitable that as the USAF continues to evolve and expand network weapon systems to increase its effectiveness in military operations, the ability to employ a dynamic change management strategy for realigning the organizational structure with environmental factors will be difficult, but essential to the successful conduct of military operations.

Bibliography

1. Air Force Communications Agency (AFCA) private web site, https://private.afca.af.mil/

2. AFCA public web site, http://public.afca.af.mil/history_pages/flares_to_satellites.pdf, p. 50.

3. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003, pp. ix.

4. Air Force Information Warfare Center (AFIWC) Mission Brief, "Delivering IO Combat Power."

5. Air Staff XCI Briefing to SAF/XC-2, *Air Force NetOps Transformation: Integrated Network Operations and Security Center (I-NOSC),* 6 July 2005.

6. Comer, Douglas E. Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition, (Upper Saddle River, New Jersey: Prentice Hall, 1995), p. 37.

7. Electronic Systems Center (ESC) home page, http://esc.hanscom.af.mil/default.asp

8. Gilder, George. "The Bandwidth Tidal Wave," *Forbes ASAP*, December 5, 1994. Located on the web at: http://www.seas.upenn.edu/~gaj1/bandgg.html

9. Government Accounting Office (GAO) Report. Information Technology Investment: A Government wide Overview (Letter Report, 07/31/95, GAO/AIMD-95-208). Letter from the Government Accounting Office to the Chairman, Committee on Governmental Affairs, U.S. Senate, July 1995. Found at URL http://www.gao.gov/archive/1995/ai95208.pdf. p. 10.

10. Gruber, Lt Col David J., USAF, *Computer Networks and Information Warfare: Implications for Military Operations*, (Occasional Paper No. 17, Center for Strategy and Technology, Air War College, Air University, Maxwell AFB, AL, July 2000)

11. Halabi, Bassam. *Internet Routing Architectures* (Indianapolis, IN: Cisco Press, New Riders Publishing, 1997), p. 3.

12. Hawley, General Richard E. Commander, Air Combat Command, 1998 speech attended by author.

13. *Information Technology Management Reform Act of 1995*, Public Law 104-208, SEC. 5125. Full text of Act located at: http://irm.cit.nih.gov/itmra/itmra96.html

14. Lagas, Robert. *Information Technology Management Reform Act Summary* (Office of Information Resources Management, National Institute of Health), at: http://www.icesa.org/articles/template.cfm?results_art_filename=itmrasum.htm

15. *Making Strategy: An Introduction to National Security Processes and Problems*, Chapter 11, August 1988, pp. 163–174. Published 1988 by Air University Press.

16. Meyerrose, Brigadier General Dale W. Air Combat Command, Director of Communications and Information, 1998.

17. Nellis Air Force Base web site, http://www.nellis.af.mil/units.htm

18. Nicholls, Colonel David J. (Vice Commander, Air Force Information Warfare Center), interview with the author, 18 November 2005

19. Rose, Marshall T. *The Simple Book: An Introduction to Management of TCP/IP based internets*, (Englewood Cliffs, New Jersey: Prentice Hall, 1991), p. xx.

20. Williams, Colonel Kent. (Deputy Director, Air Force Doctrine Center), in discussion with author, 30 November 2005.